ABSTRACT OF THE DISCLOSURE

In order to protect control programs against unauthorized analysis and use during transport via public networks, asymmetrical keys are used. Following the compilation of the control program in the engineering system belonging to the supplier, the program is encrypted in a postprocessor and exported into a public web server. The customer loads the encrypted program into his long-term data holder, imports it into his engineering system and can edit it there in order to configure the control system. Only after editing are the encrypted parts of the program decrypted in a preprocessor and forwarded to the compiler.